SYMMETRIC CRYPTOGRAPHIC ALGORITHMS FOR CLOUD ENVIRONMENT – A COMPARATIVE STUDY

Sunder V[1], Vidhya SS[2]
[1,2]Assistant Professor, Vimal Jyothi Engineering College, Chemperi, Kannur, Kerala.

ABSTRACT

Data security has become one of the most important aspect of information sharing due to the nature and types of data that we used to transfer through unsecure channels such as Internet. In Day today life we stores more private data in the cloud storage devices ever since cloud technology started its growth. The most important factor that is to be taken care while data is transferred through the Channel, is security. Cryptography is one such technique which can be used for secure transmission of the data. And, using cryptographic techniques we can provide security to the information in terms of confidentiality, in a shared communication environment. In this paper, we analyses the existing well known Symmetric cryptographic systems to identify the best performing algorithm for cloud environment by considering the trade-off between time factor and security.

Keywords: Symmetric Cryptography, cloud, performance comparison

1.1 INTRODUCTION

Cryptography is an area of computer science which is developed to provide security for the senders and receivers to transmit and receive confidential data through an insecure channel by a means of process called Encryption/ Decryption. Cryptography ensures that the message should be sent without any alterations and only the authorized person can be able to open and read the message. A number of cryptographic techniques are developed for achieving secure communication. There are basically two techniques of cryptography- Symmetric and Asymmetric. The strength of symmetric key encryption depends on the size of the key. Data can be easily decrypted if a weak key is used in the algorithm. There are various symmetric key algorithms such as DES, 3DES, AES, RSA etc. Here we are considering the mono alphabetic and transposition ciphers.

1.2 MONO ALPHABETIC CIPHER

The substitution cipher, one of the oldest forms of encryption algorithms, takes each character of a plaintext message and uses a substitution process to replace it with a new character in the Cipher text. This substitution method is deterministic and reversible, allowing the intended message recipients to reverse-substitute Cipher text characters to recover the plaintext. One particular form of substitution cipher is the Monoalphabetic Substitution Cipher, often called a “Simple Substitution Cipher". Monoalphabetic Substitution Ciphers rely on a single key mapping function K, which consistently replaces a particular character with a character from the mapping K(α). For encryption function E and decryption function D with plaintext P and Cipher text C, |P| = |C| and for all i; 0 < i _<=|P|,Ci = E(Pi) = K(Pi); Pi = D(Ci).

The mapping is one-to-one, so for all characters α,β in the plaintext,

α = β => K(α) = K(β) and α ≠ β=> K(α) 6= K(β)

Vignere Cipher

It is a commonly used Mono alphabetic cipher. One of the main problems with simple substitution ciphers is that they are so vulnerable to frequency analysis. Given a sufficiently large cipher text, it can easily be broken by mapping the frequency of its letters to the know frequencies of, say, English text. Therefore, to make ciphers more secure, cryptographers have

long been interested in developing enciphering techniques that are immune to frequency analysis. One of the most common approaches is to suppress the normal frequency data by using more than one alphabet to encrypt the message. A polyalphabetic substitution cipher involves the use of two or more cipher alphabets. Instead of there being a one-to-one relationship between each letter and its substitute, there is a one-to-many relationship between each letter and its substitutes. The *Vigenere Cipher ,* proposed by Blaise de Vigenere from the court of Henry III of France in the sixteenth century, is a polyalphabetic substitution based on the following *tableau:*

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Note that each row of the table corresponds to a Caesar Cipher. The first row is a shift of 0; the second is a shift of 1; and the last is a shift of 25. The Vigenere cipher uses this table together with a keyword to encipher a message.

For example, suppose we wish to encipher the plaintext message:

TO BE OR NOT TO BE THAT IS THE QUESTION

Using the keyword RELATIONS. We begin by writing the keyword, repeated as many times as necessary, above the plaintext message. To derive the cipher text using the tableau, for each letter in the plaintext, one finds the intersection of the row given by the corresponding keyword letter and the column given by the plaintext letter itself to pick out the cipher text letter.

Keyword:	RELAT IONSR ELATI ONSRE LATIO NSREL
Plaintext:	TOBEO RNOTT OBETH ATIST HEQUE STION
Cipher text:	KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

Decipherment of an encrypted message is equally straightforward. One writes the keyword repeatedly above the message:

Keyword:	RELAT IONSR ELATI ONSRE LATIO NSREL
Cipher text:	KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY
Plaintext:	TOBEO RNOTT OBETH ATIST HEQUE STION

This time one uses the keyword letter to pick a column of the table and then traces down the column to the row containing the Cipher text letter. The index of that row is the plaintext letter.

The strength of the Vigenere cipher against frequency analysis can be seen by examining the above cipher text. Note that there are 7 'T's in the plaintext message and that they have been encrypted by 'H,' 'L,' 'K,' 'M,' 'G,' 'X,' and 'L' respectively. This successfully masks the frequency characteristics of the English 'T.' One way of looking at this is to notice that each letter of our keyword RELATIONS picks out 1 of the 26 possible substitution alphabets given in the Vigenere tableau. Thus, any message encrypted by a Vigenere cipher is a collection of as many simple substitution ciphers as there are letters in the keyword.

Although the Vigenere cipher has all the features of a useful field cipher i.e., easily transportable key and tableau, requires no special apparatus, easy to apply.

1.3 TRANSPOSITION CIPHER

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext. That is, the order of the units is changed (the plaintext is reordered). Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.

In a columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Both the width of the rows and the permutation of the columns are usually defined by a keyword. For example, the keyword ZEBRAS is of length 6 (so the rows are of length 6), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".

In a regular columnar transposition cipher, any spare spaces are filled with nulls; in an irregular columnar transposition cipher, the spaces are left blank. Finally, the message is read off in columns, in the order specified by the keyword. For example, suppose we use the keyword ZEBRAS and the message WE ARE DISCOVERED. FLEE AT ONCE. In a regular columnar transposition, we write this into the grid as follow:

```
6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E Q K J E U
```

Providing five nulls (QKJEU) at the end. The Cipher text is then read off as:

```
EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE
```

In the irregular case, the columns are not completed by nulls:

```
6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
```

E

This results in the following cipher text:

EVLNA CDTES EAROF ODEEC WIREE

To decipher it, the recipient has to work out the column lengths by dividing the message length by the key length. Then he can write the message out in columns again, then re-order the columns by reforming the key word.

In a variation, the message is blocked into segments that are the key length long and to each segment the same permutation (given by the key) is applied. This is equivalent to a columnar transposition where the read-out is by rows instead of columns.

Columnar transposition continued to be used for serious purposes as a component of more complex ciphers at least into the 1950s.

1.4 EXPERIMENTAL RESULT AND ANALYSIS

Taking plaintext P = HELLO WORLD as example and we use:

$$K(x) = \begin{cases} M & x = D \\ V & x = E \\ I & x = H \\ F & x = L \\ J & x = O \\ K & x = R \\ R & x = W \end{cases}$$

The resulting cipher text would be C = IFVVJ FJKFM.

For simplicity, Monoalphabetic Substitution Cipher keys are typically expressed as a permutation of the 26 letters of the alphabet, such as

K = MQLDEHNWKZOAPXVUTCYISBFRGJ.

With this notation, each character in an lexicographic ordering of the letters of the alphabet maps to the character in K that shares its position,

so K(A) = M;K(B) = Q;K(C) =L….K(Z) = J.

Using this notation, K = YTUMVCLINDAFEZJBXKHPOWRQSG could represent the key in the previous example.

Frequency Graph for Monoalphabetic Cipher

Since the set of possible keys is the set of all possible permutations of the alphabet, Monoalphabetic Substitution Ciphers have a keyspace of 26!, which is over 403 septillion. If someone were able to check 1,000,000 keys per second, it would still take over 12 trillion years to check all possible keys, so cryptanalysis by brute force is infeasible. If Eve were to intercept an encrypted Cipher text C from Alice to Bob, she could relyon her knowledge of the language the message was written in and use frequency analysis. Knowing that the most common English letter, E, occurs 12.7% of the time would allow Eve to assume the most common letter in C is mapped to by E. The next most-common letters are T at 9.1%, A at 8.2%, O at 7.5%, I at 7%, N at 6.7%, and S at 6.3%. These single-letter frequencies, generally referred to as unigram frequencies, are well-known for the English language, After E, unigram frequencies are too close to each other to help, but Eve could look look beyond unigram frequencies and compare pairs and triples of letters (bigrams and trigrams, respectively), Using these frequencies, Eve can make a series of informed hypotheses about letter substitutions and test them, looking for words or phrases that she recognizes. This process is time-consuming and involves a great deal of guesswork, so the goal of any automated cryptanalysis tool should be to use this methodology to automate the process.

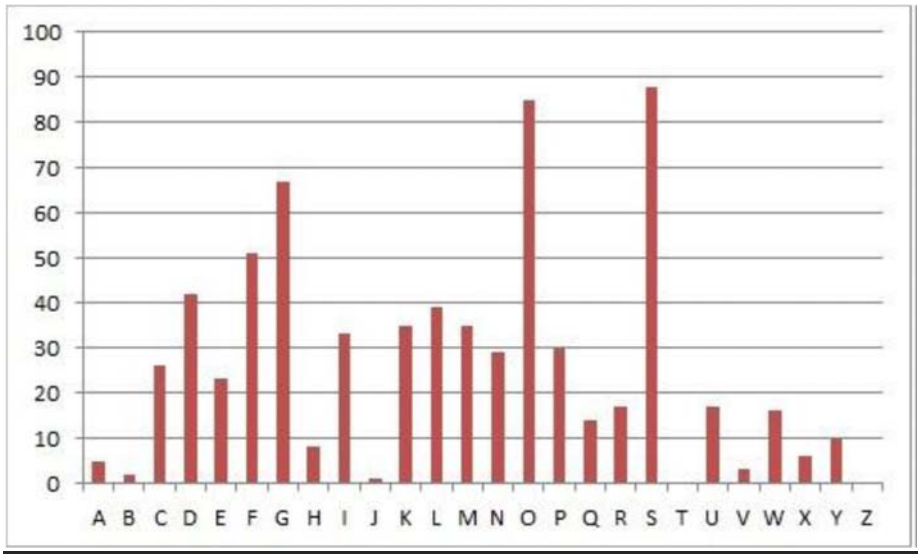

Fig 1: Monoalphabetic cipher – Frequency Graph

We used a Vigenère cipher program and the Transposition cipher runs on 32-bit operating system machine, a windows 8 enterprise, with processor Intel Core i3, with Netbeans IDE using java language . Hill cipher program is selected for examining transposition cipher. The program runs to get from the user the name of plain-text file, the key name. The program calculates the encryption and the decryption time. Then analyse the encryption and decryption according to the variable key length.

- first, we considered same length plaintext
- variable key length
- testing the result
- Then we take different key length
- variable length plain text
- observe the results
- we also tried same key length with different character
- with repetition and without
- Then analyses results and compare both ciphers based on their encryption or decryption time.

Here we take 100 inputs samples and test the results. The sample are selected as follows:

Security level	Plaintext length	Key length	Encryption & decryption time(sec)
Low	5	3	2.8
Medium	5	67	47
High	5	168	75

Column transposition cipher performance for input

Security level	Plaintext length	Key length	Encryption & decryption time(sec)
Low	5	3	10
Medium	5	67	52
High	5	130	90

- X axis- time
- Y axis- key length

Fig 2: Relationship between the performance and the key length

Fig. 1 represents the performance (the encryption time & decryption time) of the vigenere cipher and Transposition cipher for the each input. The encryption time and the decryption time increases when the key length increases.

From the analysis, the performance of Vigenere cipher and transposition cipher is better with larger key length than that of smaller key length. For more security the key length should be larger. But it is observed that encryption or decryption time varies with different keys with same key length,ie, it also depends on letter frequency. But in overall larger key length should take more time than smaller key length even though keys are different or same. Compared to both cipher transposition takes more encryption and decryption time, i.e, transposition with variable key length has more security than Vignere.

CONCLUSION

From the above experimental analysis, taking various factors into considerations, we conclude that Monoalphabetic cipher is better in terms of time. It is also understood that the key length has a vital role in the cryptographic techniques. Better study could be made by considering various other symmetric key algorithms.

REFERENCE

- Cloud Security Algorithms by Er. Ashima Pansotra and Er. Simar Preet Singh
- Efficiency of Modern Encryption Algorithms in Cloud Computing by Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem
- Comparative Study among Modern Encryption Algorithms based on Cloud Computing Environment by Dr. Box and Mohammad Farhan Hossain
- Research on cloud computing security problem and strategy by Wentao Liu
- Security issues for cloud computing by Kevin Hamlen
- Cloud Computing And Security Issues In The Cloud Monjur Ahmed and Mohammad Ashraf Hossain
- Advance cryptography algorithm for improving data security by Vishwa Gupta, Gajendra Singh, Ravindra Gupta
- Comparative Implementation of Cryptographic Algorithms on ARM Platform by Ms. Pallavi H.Dixit, Dr.Uttam L. Bombale, Mr. Vinayak B.Patil